



REC'D 13 OCT 2000

WIPO

PCT

FR00/2999

# BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

E.J.U.

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 14 SEP. 2000

**PRIORITY DOCUMENT**  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

**SIEGE**

26 bis, rue de Saint Petersburg  
75800 PARIS Cédex 08  
Téléphone : 01 53 04 53 04  
Télécopie : 01 42 93 59 30

*This Page Blank (uspto)*

26bis, rue de Saint-Petersbourg  
75800 Paris Cedex 08  
Téléphone: 01 53.04.53.04 Télécopie: 01.42.94.86.54

Code de la propriété intellectuelle-livre VI

REQUÊTE EN DÉLIVRANCE

0	RESERVE A L'INPI	
0-1	Date de remise des pièces	13.09.99
0-2	N° d'enregistrement national	99 114 95
0-3	Département de dépôt	99
0-4	Date de dépôt	13-09-1999
0-6	Titre de l'invention	Validation d'une opération au cours d'une communication entre deux terminaux à travers un réseau numérique
0-8	Etablissement du Rapport de Recherche	immédiat
0-9	Votre référence dossier	SDCNET3169
1	DEMANDEUR(s)	
1-1	Nom Adresse rue Adresse code postal et ville Pays Nationalité Forme juridique N° SIREN	FRANCE TELECOM 6, Place d'Alleray 75015, PARIS France France Société anonyme 380 129 866
2A	MANDATAIRE	
	Nom Prénom Qualité Affaire suivie par Adresse rue Adresse code postal et ville N° de téléphone N° de télécopie Courrier électronique	LAPOUX Roland CPI: 92-1136 CABINET MARTINET ET LAPOUX 43 Boulevard Vauban BP 405 - GUYANCOURT 78055, ST QUENTIN YVELINES CEDEX 01.30.64.90.09 01.30.64.90.02 martinet@wanadoo.fr
4	Déclaration de PRIORITE ou REQUETE du bénéfice de la date de dépôt d'une demande antérieure	Etat Date N° de la demande
6	Documents et Fichiers joints	Fichier électronique Pages Détails
6-1	Description	desc3169.doc 10
6-2	Revendications	rev3169.doc 3
6-3	Dessins	abr3169.doc 2
6-4	Abrégé	1
6-5	Figure d'abrégé	1
6-6	Listage de séquences	
6-7	Rapport de recherche	


<b>7</b>	<b>Mode de paiement</b>	<b>Prélèvement du compte courant</b>		
7-1	Numéro du compte client	340		
7-2	Remboursement à effectuer sur le compte n°	340		
<b>8</b>	<b>REDEVANCES</b>	Devise	Taux	Montant à payer
	062 Dépôt	FRF	250.00	250.00
	063 Rapport de recherche (R.R.)	FRF	4 200.00	4 200.00
	Total à acquitter	FRF		4 450.00
<b>10</b>	<b>Signature</b>			
10-1	Signé par	Roland LAPOUX		

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.



# BREVET D'INVENTION

## Désignation de l'inventeur

Référence utilisateur: SDCNET3169 Référence système: 111111 729823,660925926 N° d'enregistrement national:	
Titre de l'invention: Validation d'une opération au cours d'une communication entre deux terminaux à travers un réseau numérique	
Le(s) soussigné(s): Roland LAPOUX	
Désigne(nt) en tant qu'inventeur(s):	
Inventeur 1	Nom, Prénom: DUMORTIER, Jean-Paul Adresse: Rue de Secqueville F-14740 PUTOT EN BESSIN France
Inventeur 2	Nom, Prénom: HANNECART, Eric Adresse: 30, allée de la Verte Vallée Résidence G. Sand F-14000 CAEN France
Signé par:  Date: 10 sept. 1999.	

**Validation d'une opération au cours d'une  
communication entre deux terminaux à travers un  
réseau numérique**

5           L'invention concerne un procédé de validation  
d'une opération au cours d'une communication établie  
entre deux terminaux à travers un réseau numérique de  
télécommunication. Elle s'applique en particulier à  
la validation d'opérations de télépaiement par  
10 utilisation de données confidentielles, telles par  
exemple que des numéros de carte bancaire, des codes  
d'identification ou d'authentification, etc.

          Lorsque le réseau numérique de télécommunication  
est un réseau numérique à intégration de services  
15 RNIS, les terminaux d'utilisateur sont reliés à ce réseau  
par des lignes numériques bidirectionnelles qui  
transportent chacune des canaux numériques  
multiplexés comprenant au moins deux canaux logiques  
de données B et un canal logique de signalisation D.  
20 Les communications de dialogue entre terminaux  
empruntent les canaux de données B qui sont commutés  
en mode circuit, le canal D étant utilisé pour la  
signalisation usager-réseau et pouvant également  
transporter des données d'utilisateur à faible débit en  
25 mode paquet.

          Si l'on veut transmettre des données au cours  
d'une communication de conversation empruntant un  
canal de données B, il faut interrompre la  
conversation en cours entre les usagers, de sorte que  
30 la liaison est alors allouée par alternance soit à la  
conversation, soit au transport de données. Les  
données ainsi transportées ne sont pas protégées  
contre les tentatives d'interception et d'utilisation  
frauduleuse ou non autorisée.

Lorsque le réseau numérique de télécommunication utilisé est un réseau de radiotéléphonie cellulaire numérique, par exemple de type GSM, l'un des terminaux étant un radiotéléphone mobile, on  
5 rencontre également les inconvénients mentionnés ci-dessus lorsque des données doivent être échangées au cours d'une communication, celle-ci devant être interrompue pour le transport des données.

10 L'invention a notamment pour but d'éviter ces inconvénients, en utilisant au mieux les fonctionnalités des réseaux numériques de télécommunication.

15 Elle propose à cet effet un procédé de validation d'une opération au cours d'une communication établie entre des premier et deuxième terminaux à travers un réseau numérique de télécommunication, ladite communication empruntant un  
20 canal logique d'une liaison numérique multiplex comportant un autre canal logique de transport de données, caractérisé en ce qu'il comprend :

- l'établissement au cours de ladite communication, d'une liaison entre le premier  
25 terminal et un troisième terminal, via ledit autre canal de la liaison numérique multiplex,

- le transfert de données confidentielles entre le premier terminal et le troisième terminal via ledit autre canal, les données confidentielles étant  
30 destinées à la validation de l'opération effectuée au cours de la communication entre les premier et deuxième terminaux et n'étant pas accessibles au deuxième terminal ; et

- l'envoi par le troisième terminal au deuxième terminal d'un message d'acquiescement confirmant la validation de ladite opération.

5 Les données confidentielles servant à la validation de ladite opération sont donc, selon l'invention, transmises sur un canal dédié, distinct du canal utilisé pour la communication entre les premier et deuxième terminaux, sans qu'il soit nécessaire d'interrompre cette communication et sans  
10 que l'on ait un accès aux données confidentielles à partir du deuxième terminal, puisque ces données sont transmises uniquement entre le premier et le troisième terminal et indépendamment du deuxième terminal.

15

Dans un mode de réalisation préféré de l'invention, le réseau numérique de télécommunication est un réseau numérique à intégration de services RNIS et l'établissement de la liaison entre les  
20 premier et le troisième terminaux comprend l'ouverture d'un circuit virtuel dans un canal de signalisation D.

Les usagers RNIS ont en effet la possibilité de bénéficier de services de Liaison Logique Permanente (LLP) pour le transfert bidirectionnel simultané de  
25 données structurées en trames sur des canaux D de leurs accès au réseau RNIS.

A défaut, si l'utilisateur du premier terminal ne bénéficie pas des services LLP, la liaison entre les  
30 premier et troisième terminaux pour le transfert des données confidentielles peut emprunter un deuxième canal de données B de l'accès de cet utilisateur au réseau RNIS.



Selon une autre caractéristique de l'invention, le procédé comprend également l'établissement d'une liaison entre les deuxième et troisième terminaux via le réseau, demandé par le deuxième terminal, 5 préalablement à l'établissement de la liaison entre les premier et troisième terminaux, pour requérir une validation de ladite opération et ensuite pour l'envoi du message d'acquiescement par le troisième terminal au deuxième terminal.

10       Avantageusement, la liaison entre les deuxième et troisième terminaux utilise le canal de signalisation D de la ligne d'accès du deuxième terminal au réseau RNIS.

15       En variante, la liaison entre les premier et le troisième terminaux est établie à l'initiative du premier terminal, pour validation de ladite opération, et la liaison du troisième terminal avec le deuxième terminal est alors établie après cette validation, pour l'envoi d'un message d'acquiescement 20 au deuxième terminal.

L'invention prévoit également qu'une autre liaison entre les premier et deuxième terminaux puisse être établie par ouverture d'un circuit virtuel dans le canal de signalisation D, après 25 réception du message d'acquiescement par le deuxième terminal, pour le transfert de données du deuxième terminal au premier terminal. Il s'agit alors par exemple d'un téléchargement de données du deuxième terminal dans le premier terminal, suite à une 30 transaction.

Dans une variante de réalisation de l'invention, le réseau numérique de télécommunication comprend un réseau de radiotéléphonie numérique et l'établissement de la liaison entre les premier et 35 troisième terminaux utilise un service de messages

courts SMS (Short Message Service) disponible sur le réseau de radiotéléphonie.

5 L'invention s'applique, de façon générale, au commerce électronique et en particulier à une opération de télépaiement comprenant un télépaiement effectué par un usager du premier terminal au profit d'un usager du deuxième terminal et validé par les données confidentielles transférées entre les premier et troisième terminaux. Le troisième terminal est  
10 alors celui d'un établissement bancaire ou analogue, qui gère un compte de dépôt de l'usager du deuxième terminal.

L'invention s'applique également au cas où des communications entre terminaux ne peuvent être  
15 poursuivies qu'après identification ou authentification des usagers appelants, vérification de codes d'accès, etc., ces opérations d'identification, d'authentification, de vérification ou analogue étant effectuées de façon sécurisée par  
20 l'intermédiaire d'un tiers.

L'invention sera mieux comprise et d'autres caractéristiques, détails et avantages de celle-ci apparaîtront plus clairement au cours de la  
25 description qui suit, faite en référence aux dessins annexés, dans lesquels :

- la figure 1 est un bloc-diagramme schématique de plusieurs terminaux reliés par un réseau numérique mettant en œuvre une réalisation préférée du procédé  
30 selon l'invention ; et

- la figure 2 est un organigramme des opérations essentielles du procédé selon l'invention.

En figure 1, des terminaux numériques T1 et T2  
35 sont reliés à des points d'accès d'un réseau

numérique à intégration de services 10 par des lignes  
numériques bidirectionnelles 12 qui transportent des  
canaux numériques multiplexés comprenant au moins  
deux canaux de données B et un canal de signalisation  
5 D dans le cas d'un accès de base, ou bien 30 canaux  
de données B et un canal de signalisation D dans le  
cas d'un accès primaire.

Lorsque l'invention est appliquée au commerce  
électronique et au télépaiement, le terminal T1 est  
10 par exemple celui d'un client ou d'un acheteur, et le  
terminal T2 celui d'un vendeur.

La communication entre les terminaux T1 et T2  
est essentiellement une conversation, au cours de  
laquelle une opération, telle qu'un achat, est  
15 confirmée par le client.

Cette communication emprunte, suivant chacun des  
deux sens de transmission, l'un des canaux de données  
B de la ligne numérique 12.

Si le vendeur a souscrit un abonnement à un  
20 service de Liaison Logique Permanente LLP, le  
terminal T2 peut, au cours de la communication avec  
le terminal T1 du client, demander l'établissement  
d'une liaison avec un troisième terminal T3 d'un  
gestionnaire de télépaiement, tel que par exemple la  
25 banque du vendeur, par ouverture d'un circuit virtuel  
dans le canal de signalisation D. A travers la  
liaison par canal D entre les terminaux T2 et T3, le  
vendeur transmet à sa banque les caractéristiques de  
l'achat effectué par le client et comprenant  
30 notamment l'identification du client, les références  
des objets achetés et le montant total de l'achat.

Si le client a lui aussi souscrit un abonnement  
au service LLP, le terminal T3 de la banque du  
vendeur demande l'établissement d'une liaison avec le  
35 terminal T1 par ouverture d'un circuit virtuel dans

le canal de signalisation D. Une procédure de paiement utilisant des données confidentielles du client est alors mise en œuvre, cette procédure s'appuyant par exemple sur les mécanismes définis par l'Association pour le Développement du TéléPaiement (ADTP) et qui comprennent les étapes fonctionnelles suivantes :

- identification de l'objet à payer et présentation de la référence et du montant de la facture,
- présentation de l'ordre de paiement et acceptation du client,
- procédure de paiement faisant intervenir la banque du client et la banque du vendeur,
- affichage d'un certificat de prise en compte de l'ordre de paiement,
- finalisation de la transaction de paiement.

Les données confidentielles transmises entre les terminaux T1 et T3 sont inaccessibles à partir du terminal T2 du vendeur, les canaux utilisés pour les liaisons entre les terminaux T1 et T2 et entre les terminaux T1 et T3 étant distincts, même s'ils sont multiplexés dans la même ligne téléphonique numérique d'utilisateur desservant le terminal T1.

A la fin de la procédure de paiement, le terminal T3 valide le paiement par le client, en transmettant un message d'acquittement au terminal T2 à travers la liaison précédemment établie entre eux, puis rompt cette liaison en libérant le canal D correspondant, après avoir rompu la liaison par canal D avec le terminal T1.

Le vendeur ayant reçu confirmation du paiement, livre au client les objets ou articles qu'il a achetés. Lorsque ces articles ou objets sont sous forme de données numériques, le terminal du vendeur

T2 ouvre un circuit virtuel par le canal de signalisation D pour transmettre ces données au terminal de client T1.

5 Les circuits virtuels qui sont ouverts dans les canaux de signalisation D empruntent un réseau public de données commutées en mode paquet RPDCP 14 entre les deux extrémités du réseau RNIS 10 reliées aux terminaux en communication.

10 Lorsque le vendeur, le gestionnaire de télépaiement et/ou le client ne bénéficient pas des services LLP, les liaisons entre leurs terminaux empruntent uniquement des canaux de données B.

15 Le vendeur a également la possibilité lorsque son terminal T2 est en communication avec le terminal T1 du client et avec le terminal T3 du gestionnaire de télépaiement, d'établir une liaison via un deuxième canal de données B avec un terminal T4 d'un grossiste, par exemple pour se réapprovisionner.

20 Les étapes essentielles de ce procédé sont représentées dans l'organigramme schématique de la figure 2.

La première étape 16 de ce procédé établit une liaison entre les terminaux T1 et T2, empruntant un canal de données D au départ du terminal T1.

25 L'étape suivante 18 est une conversation entre les usagers de ces deux terminaux, relatif à un achat 20 par l'utilisateur du terminal T1. Pour finaliser cet achat, l'établissement d'une liaison avec le terminal T3 du gestionnaire de télépaiement est demandée par le terminal T2, en ouvrant un circuit virtuel dans un canal de signalisation D, comme indiqué en 22. Cette liaison étant établie, une demande de validation de l'achat 24 est envoyée du terminal T2 au terminal T3

30 et suivie de l'établissement d'une liaison entre ce

35

dernier et le terminal T1 du client, comme indiqué en 26, par ouverture d'un circuit virtuel dans un canal de signalisation D lorsque l'utilisateur du terminal T1 a souscrit au service LLP.

5           L'étape suivante 28 comprend le transfert de données confidentielles entre les terminaux T1 et T3, dans une mesure permettant une validation 30 de l'achat.

10           Cette validation étant acquise, le terminal T3 rompt la liaison par canal D entre celui-ci et le terminal T1, et un message d'acquiescement est envoyé du terminal T3 au terminal T2 à l'étape suivante 32 du procédé, dans la liaison précédemment établie entre les terminaux T2 et T3, qui est ensuite rompue.

15           En réponse au message d'acquiescement dans le terminal T2 confirmant le paiement de l'achat par l'utilisateur du terminal T1, l'utilisateur du terminal T2 peut alors, comme indiqué en 34, livrer ou faire livrer les objets ou articles achetés à l'utilisateur du terminal  
20           T1. Le cas échéant, cette livraison peut comprendre un téléchargement de données numériques depuis le terminal T2 dans le terminal T1, par ouverture d'un circuit virtuel dans un canal de signalisation D.

---

25           Au cours de la communication entre les terminaux T1 et T2 qui est maintenue jusqu'à la réception par le terminal T2 du message d'acquiescement, l'utilisateur du terminal T2 établit éventuellement une liaison avec le terminal T4 d'un grossiste, comme indiqué en 36, cette liaison empruntant un deuxième canal de données  
30           B d'accès du terminal T2 au réseau RNIS. A travers cette liaison, l'utilisateur du terminal T2 envoie au grossiste une demande de réapprovisionnement, comme indiqué en 38.

Dans une variante, le premier terminal T1 est un terminal radiotéléphonique mobile et l'invention est appliquée à la validation d'une opération dans une communication avec ledit terminal radiotéléphonique mobile à travers un réseau radiotéléphonique cellulaire numérique qui offre aux usagers un service de messages courts (SMS). Ces messages courts sont traités dans le réseau de radiotéléphonie comme de la signalisation et transmis par paquets indépendamment d'une communication avec le terminal radiotéléphonique. Les données confidentielles de validation de télépaiement sont alors par exemple enregistrées en mémoire EEPROM dans la carte d'identité d'utilisateur SIM incluse de manière amovible dans le terminal radiotéléphonique.

Par ailleurs, certains terminaux radiotéléphoniques disposent simultanément d'une communication téléphonique classique et d'un service GPRS (General Packet Radio Service) qui définit une architecture de réseau à commutation par paquets, le réseau GPRS pouvant être relié à des réseaux fixes de données selon la recommandation X.25, et donc à un réseau RNIS.

## REVENDICATIONS

1 - Procédé de validation d'une opération au cours d'une communication établie entre des premier et deuxième terminaux (T1, T2) à travers un réseau numérique de télécommunication (10), ladite communication empruntant un canal logique d'une liaison numérique multiplex comportant un autre canal logique de transport de données, caractérisé en ce qu'il comprend :

- l'établissement (16) au cours de ladite communication, d'une liaison entre le premier terminal (T1) et un troisième terminal (T3), via ledit autre canal de la liaison numérique multiplex,
- le transfert de données confidentielles (28) entre le premier terminal (T1) et le troisième terminal (T3) via ledit autre canal, les données confidentielles étant destinées à la validation de l'opération effectuée au cours de la communication entre les premier et deuxième terminaux (T1, T2) et n'étant pas accessibles au deuxième terminal (T2) ; et
- l'envoi par le troisième terminal (T3) au deuxième terminal (T2) d'un message d'acquiescement confirmant la validation de ladite opération.

2 - Procédé conforme à la revendication 1, caractérisé en ce que le réseau numérique de télécommunication est un réseau RNIS (10) et l'établissement de la liaison entre les premier et troisième terminaux (T1, T3) comprend l'ouverture d'un circuit virtuel dans un canal de signalisation (D).



3 - Procédé conforme à la revendication 1, caractérisé en ce que le réseau numérique de télécommunication est un réseau RNIS et la liaison entre les premier et troisième terminaux (T1, T3) emprunte un canal de données (B).

4 - Procédé conforme à l'une quelconque des revendications 1 à 3, caractérisé en ce qu'il comprend également l'établissement d'une liaison entre les deuxième et troisième terminaux (T2, T3) via le réseau (10), demandé par le deuxième terminal (T2) préalablement à l'établissement de la liaison entre les premier et troisième terminaux (T1, T3), pour requérir une validation de ladite opération et ensuite pour l'envoi du message d'acquiescement par le troisième terminal (T3) au deuxième terminal (T2).

5 - Procédé conforme à la revendication 4, caractérisé en ce que l'établissement de la liaison entre les deuxième et troisième terminaux (T2, T3) comprend l'ouverture d'un circuit virtuel dans le canal de signalisation (D).

6 - Procédé conforme à la revendication 4 ou 5, caractérisé en ce que la liaison entre les deuxième et troisième terminaux (T2, T3) et la communication entre les premier et deuxième terminaux (T1, T2) sont multiplexées dans un même support physique desservant le deuxième terminal (T2) depuis le réseau (10).

30

7 - Procédé conforme à l'une quelconque des revendications 2 à 6, caractérisé en ce qu'il comprend également, après réception du message d'acquiescement par le deuxième terminal (T2), l'établissement d'une autre liaison entre les

35

deuxième et premier terminaux (T2, T1) par ouverture d'un circuit virtuel dans un canal de signalisation (D).

5           8 - Procédé conforme à l'une quelconque des revendications 1 à 7, caractérisé en ce que le réseau numérique de télécommunication comprend un réseau de radiotéléphonie numérique et l'établissement de ladite liaison entre les premier et troisième terminaux (T1, T3) utilise un service de messages courts disponible dans le réseau de radiotéléphonie.

15           9 - Procédé conforme à l'une quelconque des revendications précédentes, caractérisé en ce que ladite opération validée au cours de la communication entre les premier et deuxième terminaux (T1, T2) comprend un télépaiement effectué par un usager du premier terminal (T1) au profit d'un usager du deuxième terminal (T2) et validé par les données confidentielles transférées entre les premier et troisième terminaux (T1, T3).

20           10 - Procédé conforme à la revendication 9, caractérisé en ce que le troisième terminal (T3) est celui d'un établissement bancaire ou analogue qui gère un compte de dépôt ouvert par l'utilisateur du deuxième terminal (T2).

FIG. 1

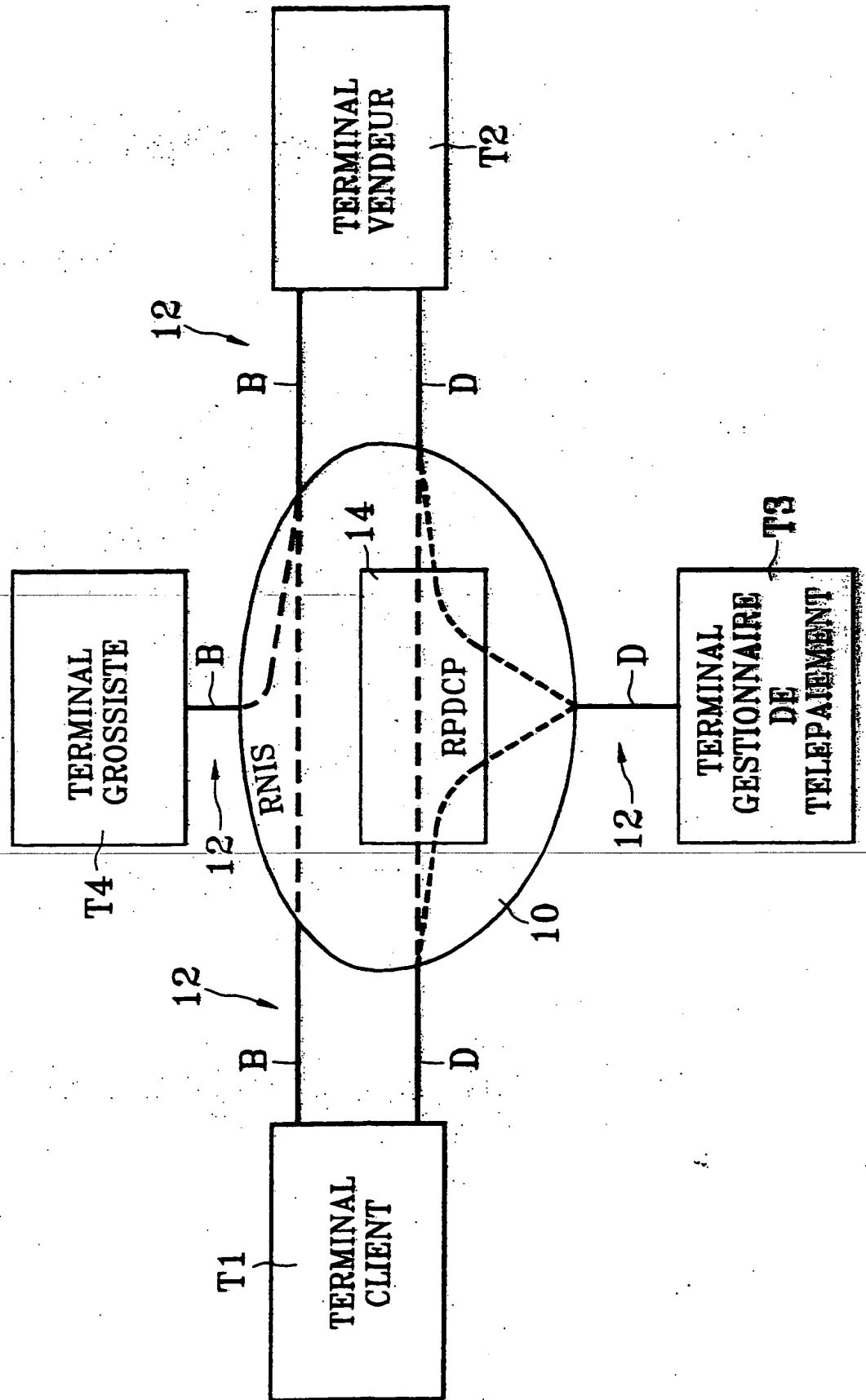


FIG. 2

